AsyncRAT, Software S1087 | MITRE ATT&CK®

Archived: 2026-04-05 13:31:43 UTC

Domain	ID		Name	Use
Enterprise	T1622		Debugger Evasion	AsyncRAT can use the `CheckRemoteDebuggerPresent` function to detect the presence of a debugger.[3]
Enterprise	T1568		Dynamic Resolution	AsyncRAT can be configured to use dynamic DNS.[4]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	AsyncRAT can hide the execution of scheduled tasks using `ProcessWindowStyle.Hidden`.[3]
Enterprise	T1105		Ingress Tool Transfer	AsyncRAT has the ability to download files over SFTP.[4]
Enterprise	T1056	.001	Input Capture: Keylogging	AsyncRAT can capture keystrokes on the victim's machine.[4]
Enterprise	T1680		Local Storage Discovery	AsyncRAT can check the disk size through the values obtained with `DeviceInfo.`[3]
Enterprise	T1106		Native API	AsyncRAT has the ability to use OS APIs including `CheckRemoteDebuggerPresent`.[3]
Enterprise	T1057		Process Discovery	AsyncRAT can examine running processes to determine if a debugger is present.[3]

Domain	ID		Name	Use
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	AsyncRAT can create a scheduled task to maintain persistence on system start-up.[3]
Enterprise	T1113		Screen Capture	AsyncRAT has the ability to view the screen on compromised hosts.[4]
Enterprise	T1033		System Owner/User Discovery	AsyncRAT can check if the current user of a compromised system is an administrator. [3]
Enterprise	T1125		Video Capture	AsyncRAT can record screen content on targeted systems.[4]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	AsyncRAT can identify strings such as Virtual, vmware, or VirtualBox to detect virtualized environments.[3]

Source: https://attack.mitre.org/software/S1087